ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

©Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2024

УДК 004.056.5

АЛГОРИТМ НАСТРОЙКИ И ПРИМЕНЕНИЯ WSL В ХОДЕ КРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА НОСИТЕЛЕЙ ИНФОРМАЦИИ

Бөлек Жандәулет Сырымұлы
zh.bolek@gmail.com
студент III курса образовательной программы 6B06306 «Системы информационной безопасности», Евразийский национальный университет им. Л. Н. Гумилева
Научный руководитель Токкулиева Айжан Конурбаевна

Защита данных становится все более критической задачей, особенно когда речь идет о флеш-накопителях [1]. В таких ситуациях методика использования Kali Linux через Windows Subsystem for Linux (WSL) выделяется как надежный и безопасный способ анализа данных на флеш-носителях.

Установка Kali Linux через WSL предоставляет ряд преимуществ. Во-первых, она позволяет создать изолированную среду для анализа данных, что минимизирует риск заражения основной операционной системы в случае обнаружения вредоносных элементов на флеш-накопителе. Кроме того, процесс установки прост и доступен даже для непрофессионалов, что делает использование Kali Linux через WSL легким и удобным.

Однако основное преимущество этой методики заключается в возможности использования инструментов The Sleuth Kit, входящих в состав Kali Linux [2,3]. The Sleuth Kit предоставляет широкий спектр утилит для анализа файловых систем и создания образов носителей данных. Эти инструменты позволяют проводить глубокий анализ флеш-накопителей, включая поиск удаленных файлов и проверку наличия вредоносных программ.

Стоит также отметить, что WSL представляет собой альтернативу виртуальным машинам, таким как VirtualBox. Однако в некоторых случаях, особенно в криминалистике, использование WSL для анализа данных на флеш-накопителях находится вне конкуренции благодаря удобству интеграции с операционной системой Windows. Это делает процесс анализа более удобным и эффективным для специалистов, работающих с данными в сфере криминалистики и цифровой безопасности.

Ниже представлен алгоритм настройки среды для дальнейшего криминалистического анализа образов носителей в Windows с помощью инструментария Linux.

Для установки Kali Linux на Windows через WSL необходимо загрузить и установить ее через Microsoft Store [4,5]. После установки необходимо прописать следующие команды в командной строке (см.рис.1):

$ sudo su	*переход в режим администратора*
# apt-get update	*обновление пакетов*
# apt-get dist-upgrade	*обновление системы*
# sudo apt install kali-win-kex	*инструменты для запуска графических приложений Windows на Kali Linux*
#kex --win -s	*запуск графической среды*

Установка Sleuth Kit на Kali Linux. The Sleuth Kit - это набор бесплатных инструментов для анализа данных на компьютере. Он помогает экспертам по безопасности и следователям извлечь информацию из жестких дисков, флэш-накопителей и других устройств хранения данных. С помощью команд fls, icat, fsstat, mactime, blkls и blkstat можно выполнять детальный анализ файловой системы на предмет извлечения цифровых улик [1,3].

Подключение флэш-накопителя к WSL. Для анализа флэш-накопителей нужно установить ряд программ:

1. usbipd-win - программное обеспечение Windows для совместного использования локально подключенных USB-устройств с другими машинами, включая гостей Hyper-V и WSL 2 [4].

2. WSL USB Manager - программа с графическим интерфейсом позволяющая управлять устройствами (рис.2) [5].

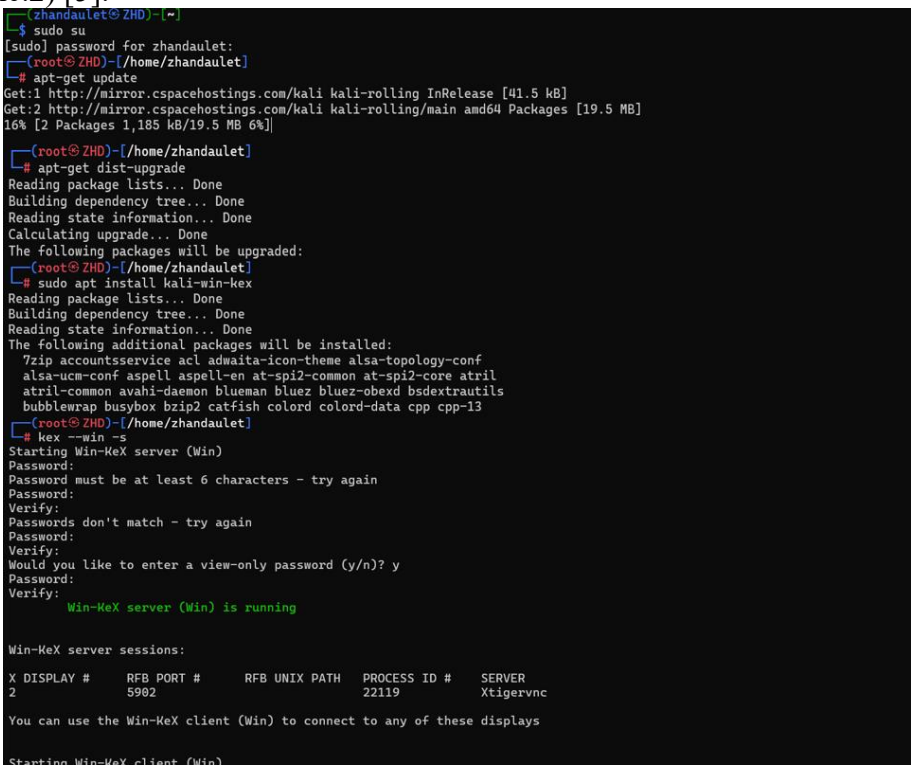

Рисунок 1. Начальная настройка WSL.

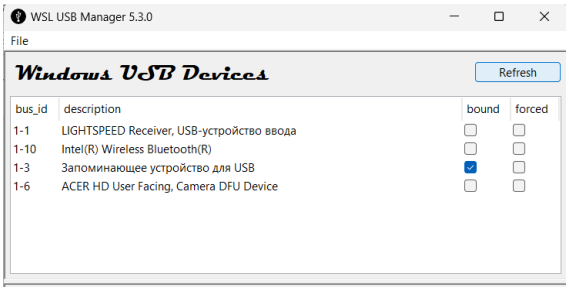

Рисунок 2. WSL USB Manager для подключения флэш накопителей к WSL.

Процесс создания образа флэш-накопителя с использованием Sleuth Kit. Для создания криминалистического образа носителя были использованы команды lsblk, dd, md5sum. Подробный пример исползования указанных команд продемонстрирован на рисунке 3.

Рисунок 3. Создание образа диска.

Анализ образа носителя и просмотр удаленных файлов. Следующие группа команд используется для детального анализа файловой системы полученного на предыдущем этапе

криминалистического образа. А именно просмотр статистики файловой системы, структура разделов и списка удаленных файлов img_stat, fsstat, fls, icat, istat, (рис. 4–8) [1,2,3].

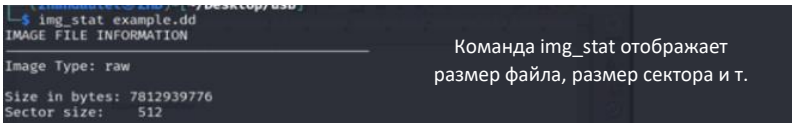

Рисунок 4. Вывод статистики образа example.dd с помощью команды img_stat

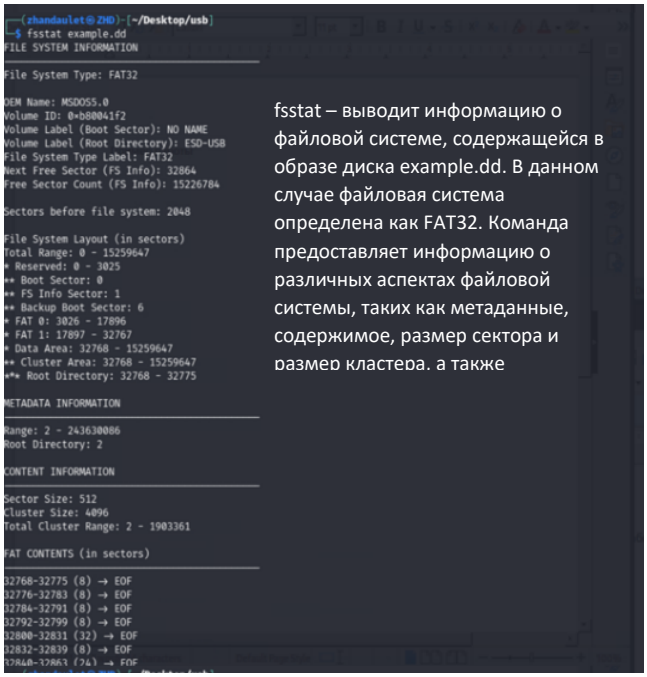

Рисунок 5. Применение команды fsstat для вывода информации о файловой системе.

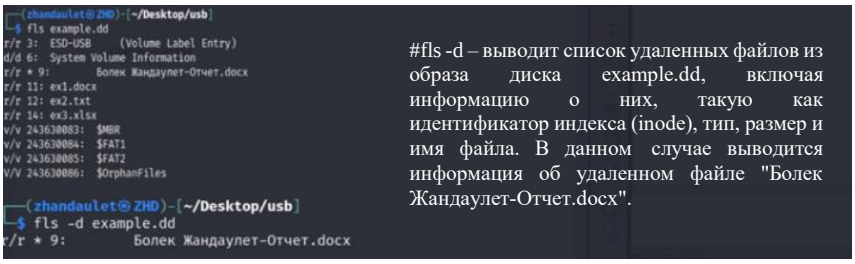

Рисунок 6. Просмотр структуры образа носителя и вывод удаленных файлов.

Рисунок 7. Восстановление удаленного файла с помощью icat.

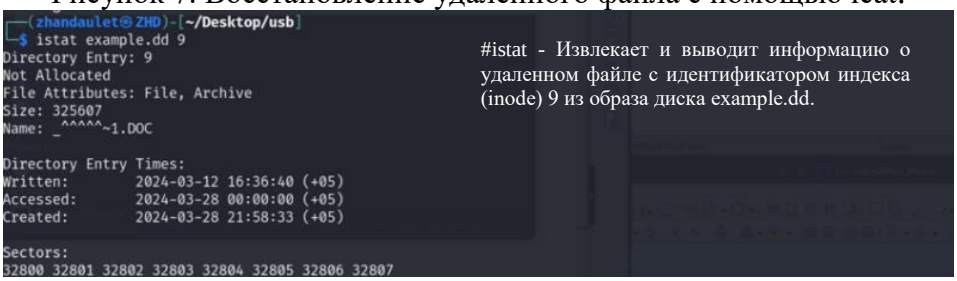

Рисунок 8. Анализ файловой системы исследуемого носителя.

В ходе анализа криминалистического образа носителя был восстановлен ранее удаленный файл, сделан детальный анализ файловой системы носителя и получена статистика носителя информации, необходимой в дальнейшем анализе.

Преимущества использования Kali Linux через WSL для анализа флэш-накопителей очевидны и играют ключевую роль в обеспечении безопасности данных. Во-первых, этот подход гарантирует изоляцию среды анализа, что снижает риск заражения основной операционной системы в случае обнаружения вредоносных элементов на флэш-накопителе. Во-вторых, установка и настройка Kali Linux через WSL просты и доступны даже для неопытных пользователей. Благодаря этому, широкий круг пользователей может воспользоваться мощными инструментами, такими как Sleuth Kit, который значительно упрощает создание образов флэш-накопителей и анализ удаленных данных.

Применение методики использования Kali Linux через WSL в анализе флэш-накопителей предоставляет пользователям возможность эффективно выявлять потенциальные угрозы безопасности и принимать соответствующие меры для защиты данных. Этот подход не только обеспечивает безопасность и конфиденциальность информации, но и повышает уверенность пользователей в целостности и надежности их данных.

Необходимо отметить, что создание образа флэш-накопителя с помощью утилиты dd играет ключевую роль в процессе анализа. Создание образа позволяет сохранить целостность оригинальных данных, обеспечивая более точный и надежный анализ. Таким образом, использование Kali Linux через WSL открывает новые возможности для безопасного анализа флэш-накопителей и обеспечения защиты данных в цифровой среде с использованием Windows.

Список использованных источников

1. Oh J., Lee S., Hwang H. Forensic recovery of file system metadata for digital forensic investigation //IEEE Access. – 2022. – Т. 10. – С. 111591-111606.

2. Easttom C. Digital Forensics, Investigation, and Response. – Jones & Bartlett Learning, 2021.

3. Nikkel B. Practical Linux Forensics: A Guide for Digital Investigators. – no starch Press, 2021.

4. https://github.com/dorssel/usbipd-win/ - Windows software for sharing locally connected USB devices to other machines, including Hyper-V guests and WSL 2.

5. https://gitlab.com/alelec/wsl-usb-gui - WSL USB Manager to manage connecting USB devices from Windows to the WSL linux environment.

УДК 004.056.5

БОРЬБА С АКАДЕМИЧЕСКОЙ НЕЧЕСТНОСТЬЮ: ВНЕДРЕНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ В СИСТЕМЫ УПРАВЛЕНИЯ ОБУЧЕНИЕМ ДЛЯ ПРЕДОТВРАЩЕНИЯ ФАЛЬСИФИКАЦИИ ДАННЫХ

Данияров Олжас Адылканович
olzhas.danayarov@mail.ru
Евразийский национальный университет имени Л. Н. Гумилёва
Научный руководитель старший преподаватель Аймичева Г.И.

Академическая нечестность, включая практику "buddy punching" и представление чужих работ, становится все более распространенной и серьезной проблемой в образовательной среде. Это явление подрывает целостность систем оценки, а также влияет на принципы справедливости и меритократии, лежащие в основе академического сообщества. В данном контексте внедрение метода двухфакторной аутентификации (2FA), основанного на использовании QR-кодов и одноразовых паролей (OTP), в системы управления обучением (LMS) представляет собой важный шаг в борьбе с академической нечестностью. Использование 2FA для входа в систему значительно усложняет возможность злоупотребления системой и представления чужих действий как своих собственных. Этот